REMARKS/ARGUMENTS

This Amendment is in response to the Office Action mailed July 24, 2007. Claims 1-19 were pending in the present application. This Amendment amends claims 1, 2, 4-6, 9, and 15, cancels claim 3 without prejudice, and adds new claims 20 and 21, leaving pending in the application claims 1, 2, and 4-21. Reconsideration of the rejected claims is respectfully requested.

35 U.S.C. §102(e) Rejection of Claims 1 and 3-19

Claims 1 and 3-19 are rejected under 35 U.S.C. §102(e) as being anticipated by Rayes et al. (U.S. Patent No. 7,234,163, hereinafter "Rayes"). Applicant respectfully submits that Rayes does not disclose each and every feature of the claims.

Claims 1 and 3-8

Independent claim 1, as amended, recites:

> A method for detecting ARP spoofing in a computer network, the method comprising:
>
> receiving a data packet at an ARP collector, wherein the data packet is generated by a first device on the network, and wherein the data packet includes information from an ARP reply received at the first device from a second device on the network, the information including a MAC address of the second device and an IP address given as a source IP address of the second device in the ARP reply; and
>
> analyzing at least one association in a database accessible to the ARP collector to determine when ARP spoofing occurs, wherein the analyzing is based on a time associated with the at least one association, and wherein the at least one association includes a MAC address that is identical to the MAC address included in the data packet.
>
> (Applicant's claim 1, as amended; emphasis added).

Applicant submits that at least the above-recited features are not disclosed by Rayes.

As best understood, Rayes is directed to a specific technique for identifying spoofing of network addresses in which a database (*i.e.*, NMS Database 170 of Fig. 1) maintains authoritative, or non-spoofable, [MAC address, IP address, port ID] bindings for network devices. (*See* Rayes: col. 3, lines 43-49; col. 6, lines 32-34; Fig. 1). At a time an ARP reply is received, the source MAC address, source IP address, and source port for the ARP reply is checked against the bindings stored in the NMS database. If the source MAC address, source IP address, and source port does not match a stored binding, the ARP reply is determined to be a spoofed reply. (Rayes: col. 7, line 27 – col. 9, line 4; Figs. 4A-4C).

Applicant submits that the invention of Rayes is substantially different from the claimed embodiments of the present invention. For example, Rayes does not teach anything about analyzing at least one association in a database to determine when ARP spoofing occurs, "wherein the analyzing is based on a time associated with the at least one association" as recited in amended claim 1. As described above, the invention of Rayes determines when ARP spoofing occurs by simply checking the source MAC address, source IP address, and source port ID for an ARP reply against a database of authoritative [MAC address, IP address, port ID] entries. Rayes makes absolutely no reference to performing ARP spoofing analysis based on a time associated with an association in a database. Accordingly, Rayes fails to disclose "wherein the analyzing is based on a time associated with the at least one association" as recited in amended claim 1.

For at least the foregoing reason, Applicant respectfully submits that Rayes does not anticipate or render obvious Applicant's claim 1, and requests that the rejection of claim 1 be withdrawn.

Dependent claims 4-8 depend from independent claim 1, and are thus believed to be allowable for at least a similar rationale as discussed for claim 1, and others. Accordingly, Applicant respectfully requests that the rejection of these dependent claims be withdrawn.

Dependent claim 3 has been canceled without prejudice. Accordingly, the rejection of claim 3 is believed to be moot.

Claims 9-14

Independent claim 9, as amended, recites:

> In an ARP collector a method for detecting ARP spoofing, the method comprising:

> receiving ARP Tunnel Protocol (ATP) packets from a first subnet of a computer network;
>
> receiving ATP packets from a second subnet of the computer network;
>
> storing information from the ATP packets from the first subnet in a database of the ARP collector;
>
> storing information from the ATP packets from the second subnet in the database of the ARP collector; and
>
> analyzing the received ATP packets and information in ARP collector database to determine when a spoofed ARP reply has been received on a port of the computer network.
>
> (Applicant's claim 9, as amended; emphasis added).

Applicant submits that at least the above-recited features are not disclosed by Rayes.

For example, Rayes does not disclose "receiving ARP Tunnel Protocol (ATP) packets from a first subnet of a computer network," "receiving ATP packets from a second subnet of the computer network," and "analyzing the received ATP packets. . . to determine when a spoofed ARP reply has been received" as recited in claim 9. (Emphasis added). The Office Action asserts that these features are shown in Rayes at col. 5, lines 41-50, col. 7, lines 35-41, and Fig. 1, reference numerals 140A, 160, and 170. (Office Action: pg. 3). Applicant respectfully disagrees.

As an initial matter, Applicant submits that the cited sections of Rayes do not teach anything about receiving an ARP Tunnel Protocol (ATP) packet, which is defined in the Specification as a packet type that is particularly adapted for transmitting ARP reply information to a centralized ARP collector. (Specification: pg. 8, lines 12-22). Col. 5, lines 41-50 of Rayes describe receiving a DHCP request at a Layer 2 switch from a host network device. However, as is well known in the art, a DHCP request is merely a mechanism for requesting a dynamic IP address from a DHCP server. Applicant submits that the DHCP request described in Rayes is completely unrelated to the recited ATP packet of claim 9.

Col. 7, lines 35-41 of Rayes describe receiving an ARP message (*i.e.*, ARP reply) at a Layer 2 switch from a host network device. However, as is well known in the art, an ARP message/reply is merely a mechanism for identifying a source MAC address for a source IP address. Like the DHCP request discussed above, the ARP message/reply described in Rayes is completely unrelated to the recited ATP packet of claim 9.

Even *assuming arguendo* that Rayes could be construed as teaching the step of receiving ATP packets, Rayes makes no reference (and the Examiner provides no citation) to the concept of receiving ATP packets from first and second subnets of a network as recited in claim 9. Further, since Rayes does not teach anything about receiving ATP packets from first and second subnets, Rayes necessarily fails to disclose or even suggest "analyzing the received ATP packets. . . to determine when a spoofed ARP reply has been received" as recited in claim 9.

For at least the foregoing reasons, Rayes does not anticipate or render obvious Applicant's claim 9. Accordingly, Applicant respectfully requests that the rejection of claim 9 be withdrawn.

Dependent claims 10-14 depend from independent claim 9, and are thus believed to be allowable for at least a similar rationale as discussed for claim 9, and others. Accordingly, Applicant respectfully requests that the rejection of these dependent claims be withdrawn.

Claims 15-19

Independent claim 15 has been amended to recite features that are substantially similar to independent claim 1, and is thus believed to be allowable for at least a similar rationale as discussed for claim 1, and others. Accordingly, Applicant respectfully requests that the rejection of claim 15 be withdrawn.

Dependent claims 16-19 depend from independent claim 15, and are thus believed to be allowable for at least a similar rationale as discussed for claim 15, and others. Accordingly, Applicant respectfully requests that the rejection of these dependent claims be withdrawn.

35 U.S.C. §103(a) Rejection of Claim 2

Claim 2 is rejected under 35 U.S.C. §103(a) as being unpatentable over Rayes in view of Gunter et al. (U.S. Patent No. 6,751,728, hereinafter "Gunter"). Applicant respectfully submits that Rayes and Gunter, considered individually or in combination, do not teach or suggest the features of this claim.

Claim 2 depends from independent claim 1. Thus, claim 2 is believed to be allowable over Rayes for at least a similar rationale as discussed for claim 1, and others.

The deficiencies of Rayes in this regard are not remedied by Gunter. Gunter is directed to a technique for transmitting encrypted packets from a sending host in an external network to a receiving host on an intranet through a network access point. (Gunter: Abstract). As best understood, Gunter makes no reference to, for example, "analyzing at least one association in a database accessible to the ARP collector to determine when ARP spoofing occurs, wherein the analyzing is based on a time associated with the at least one association" as recited in claim 1.

Thus, even if Rayes and Gunter were combined (although there appears to be no rationale for combining), the resultant combination would not teach or suggest all of the features of claim 2. Accordingly, Applicant respectfully submits that claim 2 is allowable over the combination of Rayes and Gunter, and requests that the rejection of claim 2 be withdrawn.

Newly Presented Claims 20 and 21

Claim 20 and 21 have been added to cover different aspects of the present invention. These claims are supported by the Specification as filed and do not add new matter.

Independent claim 20 recites, in part "analyzing at least two associations in a database accessible to the ARP collector to determine when ARP spoofing occurs, wherein each of the at least two associations include a MAC address that is identical to the MAC included in the data packet." Applicant submits that Rayes and Gunter make no reference to analyzing at least two associations in a database to determine when ARP spoofing occurs, where each of the at least two association include a MAC address that is identical to the MAC address included in a received data packet. Accordingly, claim 20 is believed to be patentable over Rayes and Gunter for at least this reason.

Dependent claim 21 depends from independent claim 1, and is thus believed to be allowable for at least a similar rationale as discussed for claim 1.

Further, Applicant submits that claim 21 recites additional features that distinguish over Rayes and Gunter. For example, claim 21 recites, in part:

> identifying a second association in the database, wherein the second association includes a MAC address that is identical to the MAC address of the first association, an IP address that is identical to the IP address of the first association, and a second time;
>
> identifying a third association in the database, wherein the third association includes a MAC address that is identical to the MAC address of the first association, an IP address that is different from the IP address of the first association, and a third time subsequent to the second time; and
>
> determining when ARP spoofing occurs based on whether the first, second, and third times fall within a predefined time interval.
>
> (Applicant's claim 21, in part).

Applicant submits that Rayes and Gunter make no reference to the above-recited features of claim 21. Accordingly, claim 21 is believed to be allowable over Rayes and/or Gunter for at least this additional reason.

Amendments to the Claims

Unless otherwise specified, amendments to the claims are made for purposes of clarity, and are not intended to alter the scope of the claims or limit any equivalents thereof. The amendments are supported by the Specification as filed and do not add new matter.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 650-326-2400.

Respectfully submitted,

/Andrew J. Lee/

Andrew J. Lee
Reg. No. 60,371

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 650-326-2400
Fax: 415-576-0300
AJL:mg
61125732 v1